



FORGEROCK™

An Introduction to User-Managed Access (UMA)

Eve Maler

VP Innovation & Emerging Technology

eve.maler@forgerock.com

[@xmlgrri](https://twitter.com/xmlgrri)

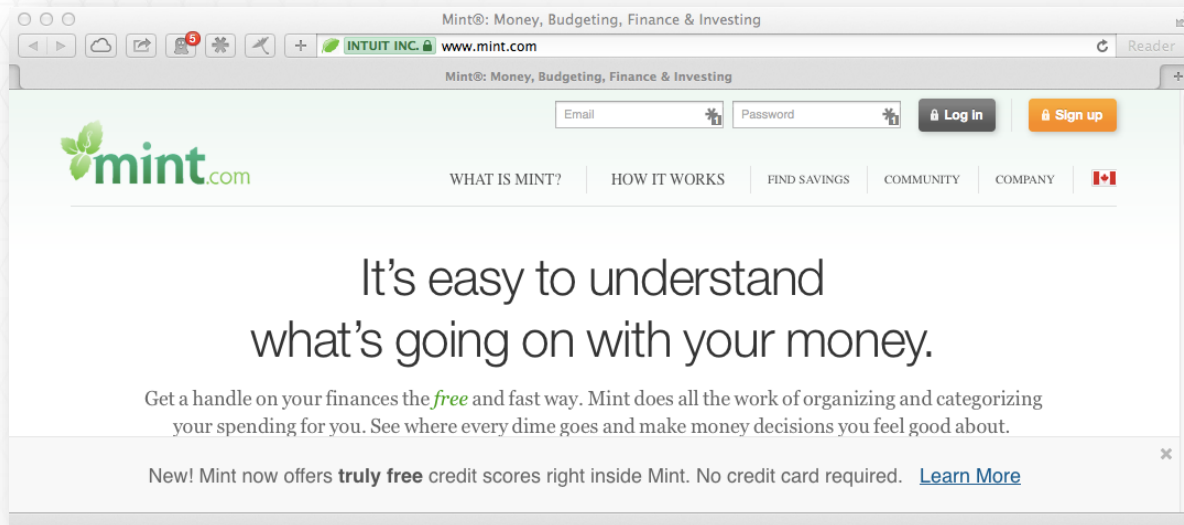
February 9, 2015

Some apps are still in the Web 1.0 dark ages

- Provisioning user data by hand
- Provisioning it by value
- Oversharing
- Lying!

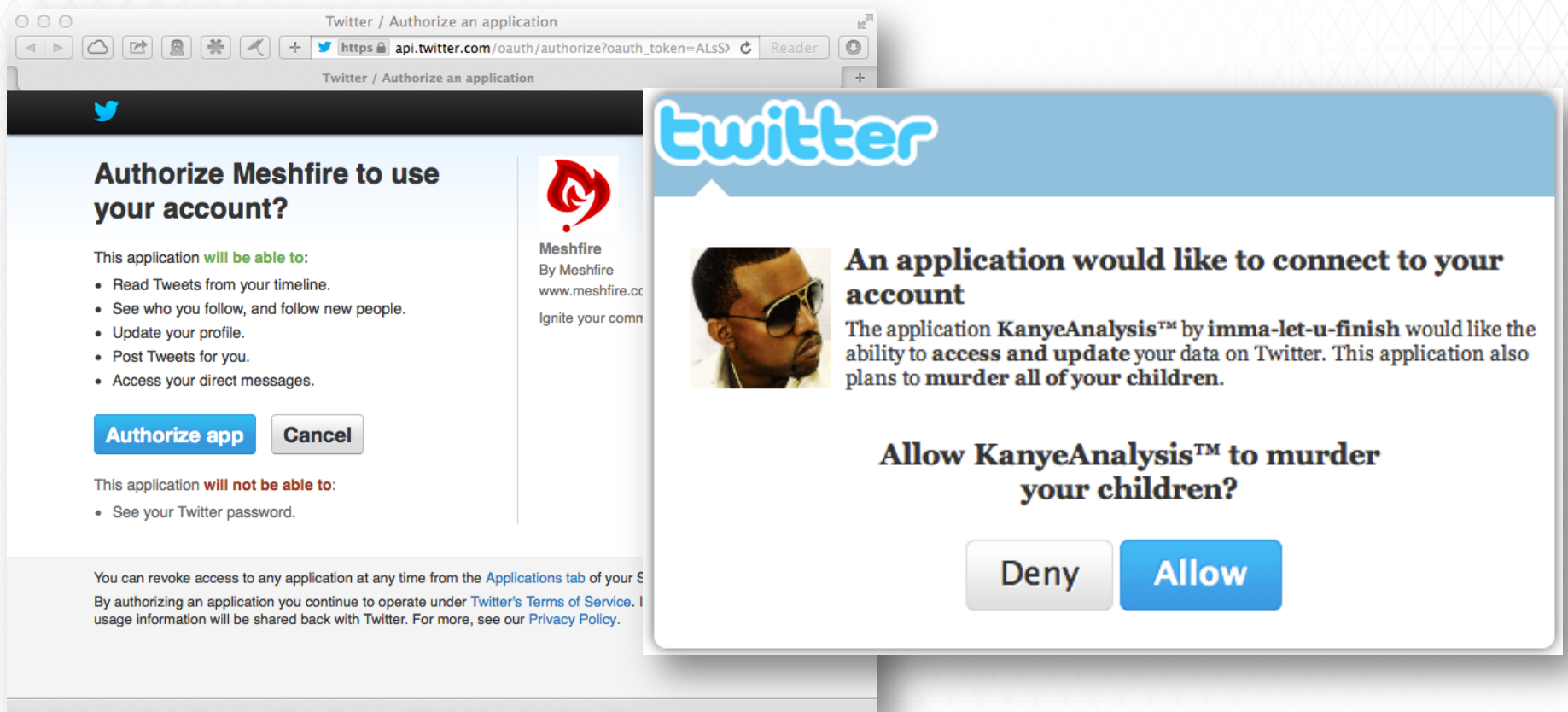
Name	<input type="text"/>
Street Address	<input type="text"/> <input type="text"/>
City	<input type="text"/>
State	<input type="text" value="Enter Text"/> ▼
Zip/Postal	<input type="text"/> <input type="text"/>
Province	<input type="text"/>
Country	<input type="text" value="Enter Text"/> ▼
Phone	<input type="text"/>
Email	<input type="text"/>
Preferred Communication	<input type="radio"/> Postal Mail <input type="radio"/> Phone <input type="radio"/> E-mail

Some other apps are still in the Web 2.0 dark ages



- The “password anti-pattern” – a third party impersonates the user
- It’s a honeypot for shared secrets
- B2B partners are in the “gray market”

Apps using OAuth and OpenID Connect hint at a better, if not perfect, way



What about selective *party-to-party* sharing?

Vancouver, WA, September 2014


Sep 24 - 26, 2014 / Vancouver, WA

Travelers:

Viewers:

Planners:

Tripit
from Concur



Here Comes the Sun choreo - Google Docs

https://docs.google.com/document/d/1ISWPDnck1K_epT4fTJ2EjEWfzEoCKzoOSM8y-BoXU/edit#heading=h.j Reader

Here Comes the Sun choreo - Google Docs

Here Comes the Sun choreo ☆

File Edit View Insert Format Tools Table Add-ons Help Last edit was made on August 19, 2013 by Mindy Engelberg Comments

xmlgrl@gmail.com

100% Title Trebuchet ... 21 B I U A

1 2 3 4 5 6 7

Your account / Allow printing

flickr

Flickr has partnered with Snapfish to bring you international printing! You can now use your Flickr photos to make prints, create posters, photo books and more from anywhere in the world.

Who can print your photos

Don't forget to make sure that you have all the necessary rights and you won't be infringing on any third parties with any content that you license on Flickr. As per our [Community Guidelines](#), accounts are intended for members to share content that they themselves have created.

Our choices: send a private URL....

- Handy but insecure
- Unsuitable for really sensitive data



...or require impersonation...

Import Fidelity Tax Information Into TurboTax®

If you are a Fidelity customer and use TurboTax®, you may be able to import certain information directly from your account into the software. Here's how.

How to import your information

Once you receive your 1099 statement by mail or through eDelivery, have it available to verify the imported information. Follow these simple steps:





1. Enter your Social Security number (SSN), taxpayer identification number (TIN), or username, and then your password. When asked where to import information from, select Fidelity Investments and enter the same information that you use to log on to Fidelity.com. Then, the tax information available for each of the accounts associated with your SSN should appear.

...or
implement a
proprietary
access
management
system


Sharing settings


Link to share (only accessible by collaborators)


https://docs.google.com/document/d/1ISWPDnkck1K_epT4fJTj2EjEWfzEoCKzoOSM/


Share link via:    

Who has access

 Specific people can access [Change...](#)

 Eve Maler (you) xmigr1@gmail.com Is owner

 Kat E [Can edit](#) ×

 Mindy Engelberg

[Is owner](#)

☒ [Can edit](#)

[Can comment](#)

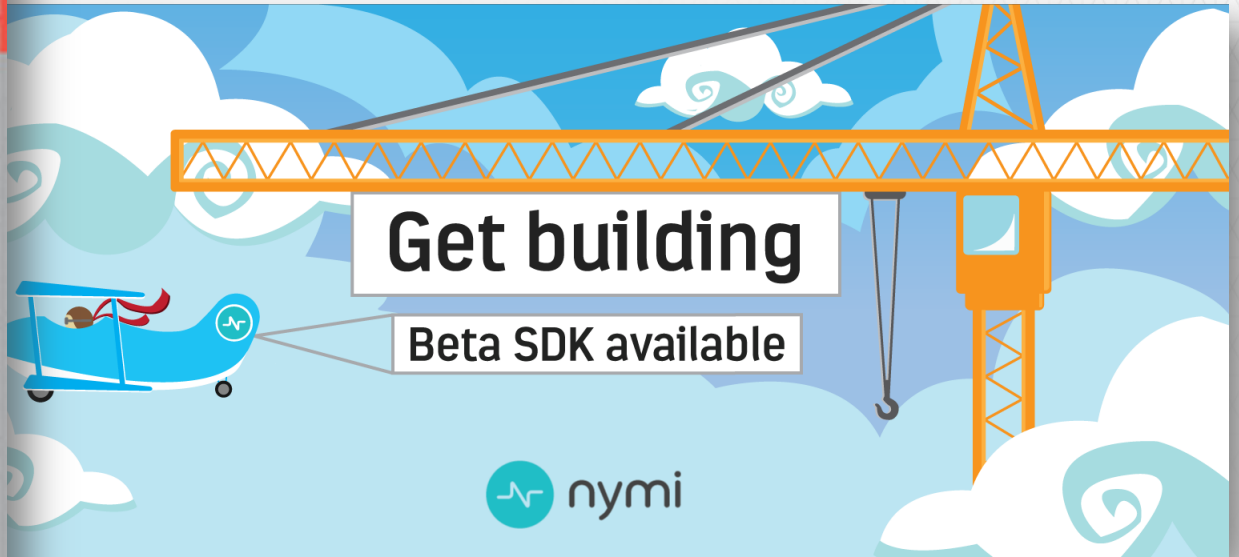
[Can view](#)

Invite people:

Editors will be allowed to add people and change the permissions. [\[Change\]](#)

[Done](#)

Killing – or even *wounding* – the password kills impersonation



IoT 2.0 is here – and it too needs authorization

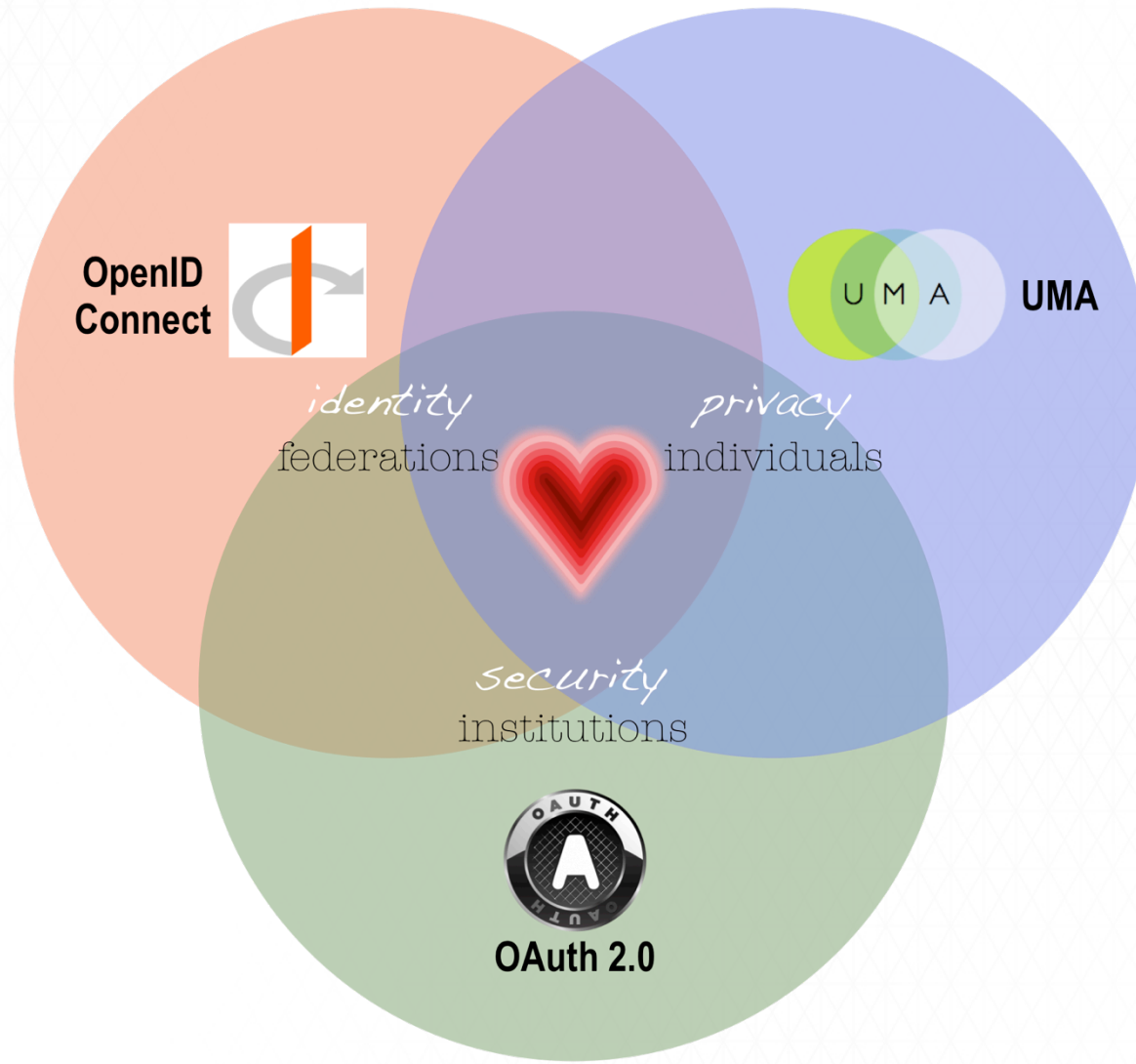


We have tough requirements for delegated authorization

- Lightweight for developers
- Robustly secure
- Privacy-enhancing
- Internet-scalable
- Multi-party
- Enables end-user convenience



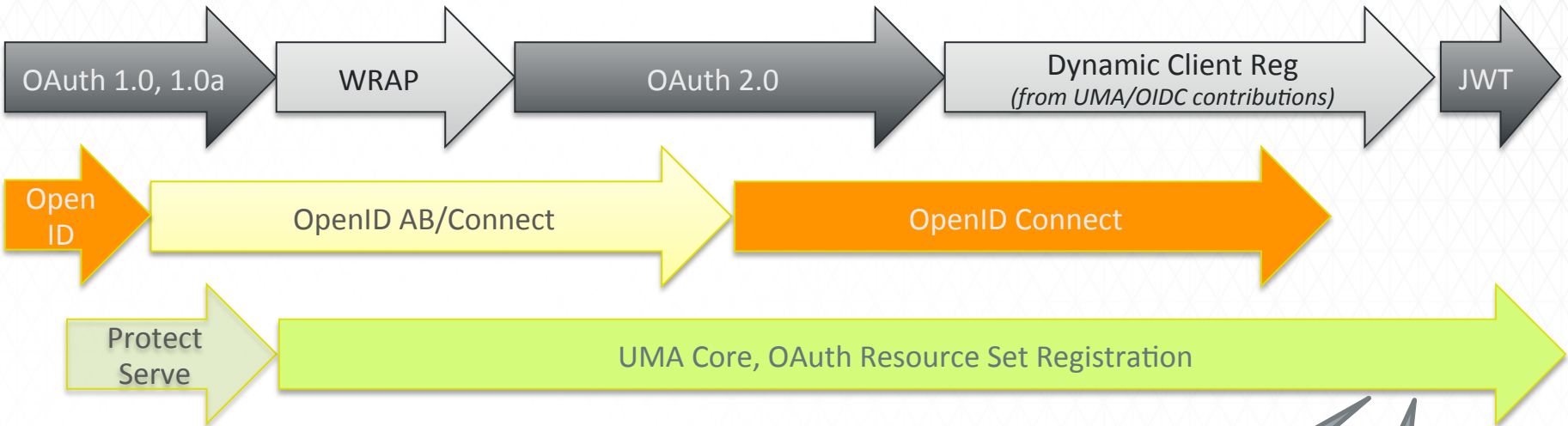
The new Venn of access control



UMA protocol standardization in context



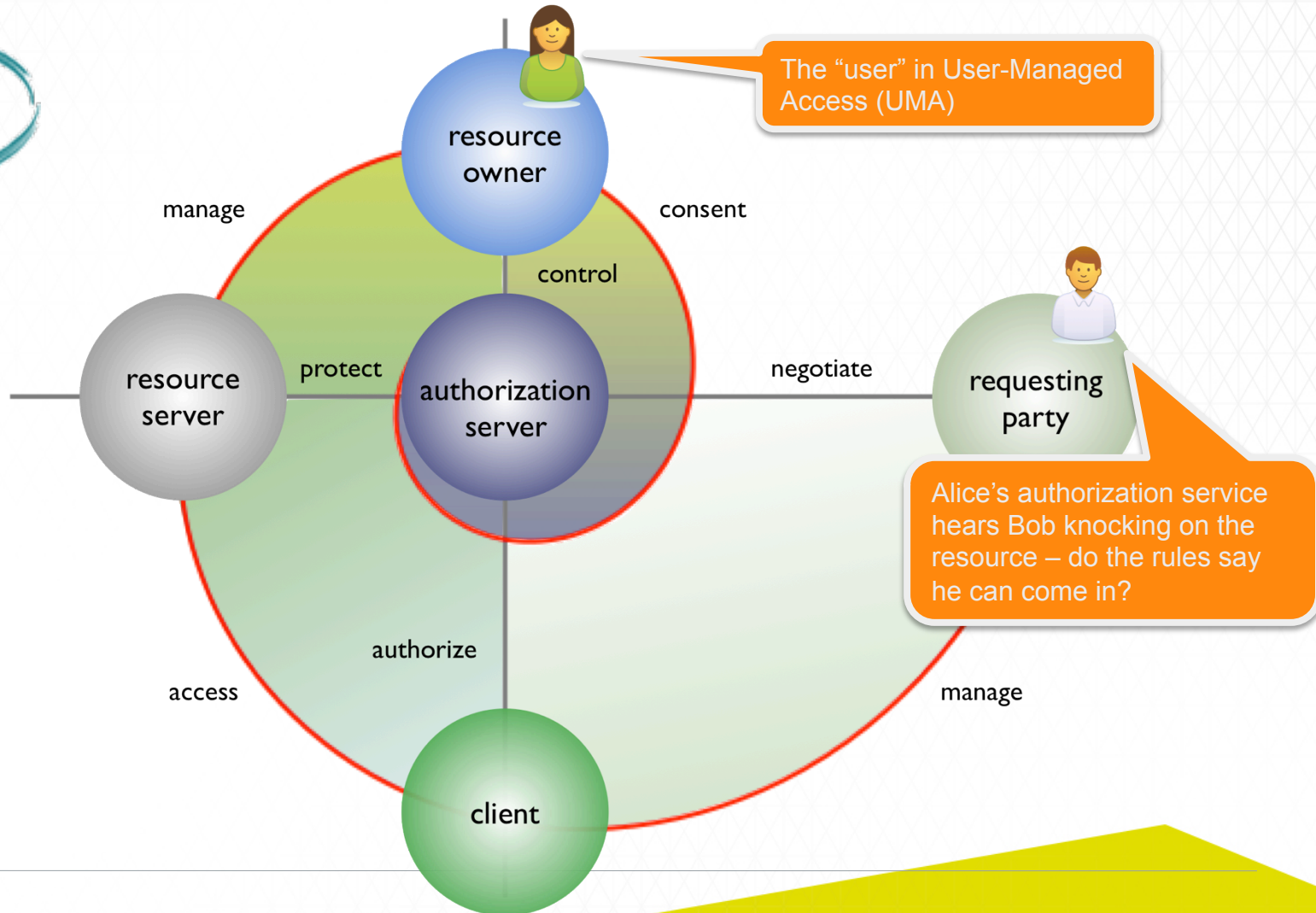
08 09 10 11 12 13 14 15



5 Jan '15: 45-day public review of "V1.0 candidate" specs begun: tinyurl.com/umacore & oathrsr

Interop test suite development under way

UMA turns online sharing into a Privacy-by-Design solution



UMA-enabled systems can respect policies such as...

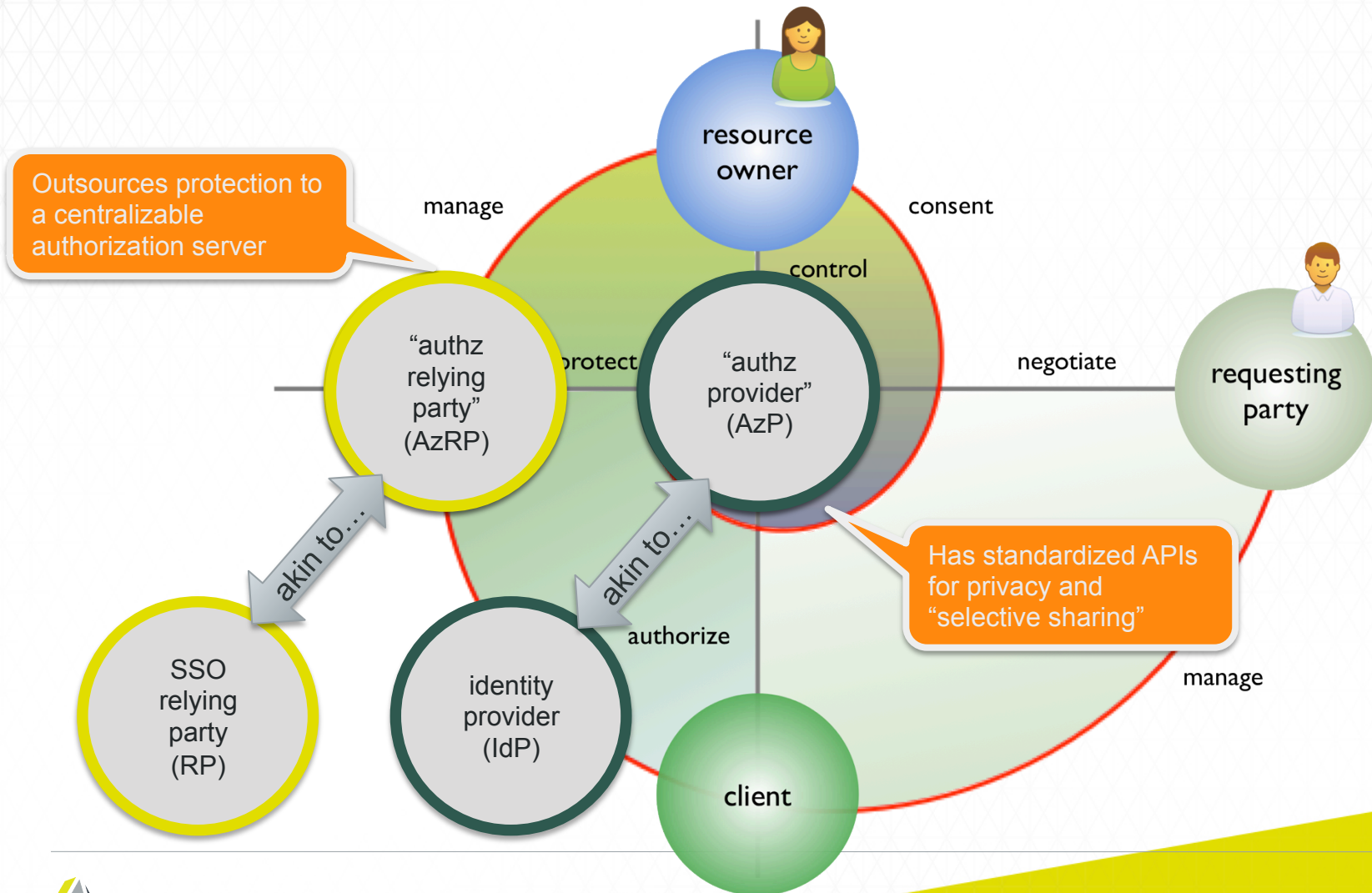
Only let my tax preparer with email TP1234@gmail.com and using client app **TaxThis** access my **bank account data** if they have **authenticated strongly**, and **not after tax season is over**.

Let my **health aggregation app**, my **doctor's office client app**, and the client for my husband's employer's **insurance plan** (which covers me) get access to my **wifi-enabled scale API** and my **fitness wearable API** to **read** the results they generate.

When a person driving a vehicle with an **unknown ID** comes into contact with my **Solar Freakin' Driveway**, alert me and **require my access approval**.



UMA is about interoperable, RESTful authorization-as-a-service



Use-case scenario domains

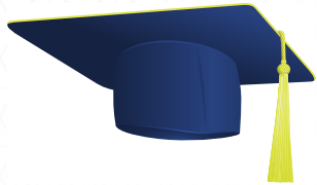


Health

Financial



Education



Personal



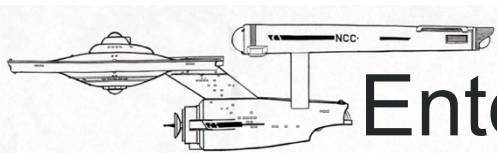
Government



Media



Enterprise



Web

Mobile



API

IoT



Introducing the OpenUMA community open-source project

The screenshot shows a web browser window displaying the OpenUMA community page. The browser's address bar shows the URL `forgerock.org/openuma/`. The page header includes the ForgeRock logo and navigation links: [Blog](#), [Projects](#), [Documentation](#), [Downloads](#), [Resources](#), [Forums](#), [Events](#), and a search icon. A user profile icon is visible with links for [Live Notifications](#), [Your activity](#), [Site activity](#), [Settings](#), and [Log Out](#). The main content area is titled "OpenUMA" with a subtitle "Home / OpenUMA". A green banner at the top of the content area says "Check out OpenAM 12 and Social Authentication!". The main text area contains the heading "OpenUMA" followed by a paragraph: "You know that blue 'Share' button in Google Apps? Ever wanted to add a feature like that to your own app or API ecosystem? The UMA protocol enables you to do just that." Below this is a paragraph explaining User-Managed Access (UMA) as an OAuth-based protocol. To the right, under the heading "On this page:", there is a list of links: [About the UMA Standard](#), [Project goals](#), [Sample Use Case](#), [Infographic: UMA](#), [The OpenUMA video](#), [OpenUMA blog posts](#), and [Get involved!](#). Further right, under the heading "Leaderboard", there is a list of top contributors: #1 Peter Major (405), #2 Victor Ake (398), #3 Brad Tomy (350), #4 Scott Heger (342), #5 David G. Simmons (341), and #14 Eve Maler (147). Below the leaderboard, a note states: "The leaderboard is based on our rockin' informal points system, read about it [here](#)." At the bottom right, under the heading "Recently Active Members", there are four profile icons. At the very bottom of the page, there is a footer with the text "THE UMA STANDARD EXPLAINED".

OpenUMA - ForgeRock Community

FORGEROCK

OpenUMA
Home / OpenUMA

Check out OpenAM 12 and Social Authentication!

OpenUMA

You know that blue "Share" button in Google Apps? Ever wanted to add a feature like that to your own app or API ecosystem? The UMA protocol enables you to do just that.

User-Managed Access (UMA) is an OAuth-based protocol that enables an individual to control the authorization of data sharing and service access made by others.

The OpenUMA community shares an interest in informing, improving, and extending the development of UMA-compatible open-source software as part of ForgeRock's Open Identity Stack. Currently no open-source OpenUMA code has yet been published, but keep an eye out in early 2015!

On this page:

- [About the UMA Standard](#)
- [Project goals](#)
- [Sample Use Case](#)
- [Infographic: UMA](#)
- [The OpenUMA video](#)
- [OpenUMA blog posts](#)
- [Get involved!](#)

Leaderboard

- #1 [Peter Major](#) 405
- #2 [Victor Ake](#) 398
- #3 [Brad Tomy](#) 350
- #4 [Scott Heger](#) 342
- #5 [David G. Simmons](#) 341
- #14 [Eve Maler](#) 147

The leaderboard is based on our rockin' informal points system, read about it [here](#).

Recently Active Members

THE UMA STANDARD EXPLAINED

Demo

Summary of your 2013 Wages and Taxes

🔒 Share Your W-2

📄 Download Your W-2



EMPLOYEE DETAILS

ALICE M SM
1234 FLORA
SAN FRANC
CA 94401



EMPLOYER DETAILS

Share with others

People

bob@gmail.com ✕

People you share this with will be required to have a valid ID if they don't have one and you will be able to revoke access

Basic Authentication ▾

- ✓ Basic Authentication
- Two-step Authentication



Done

Settings

\$999

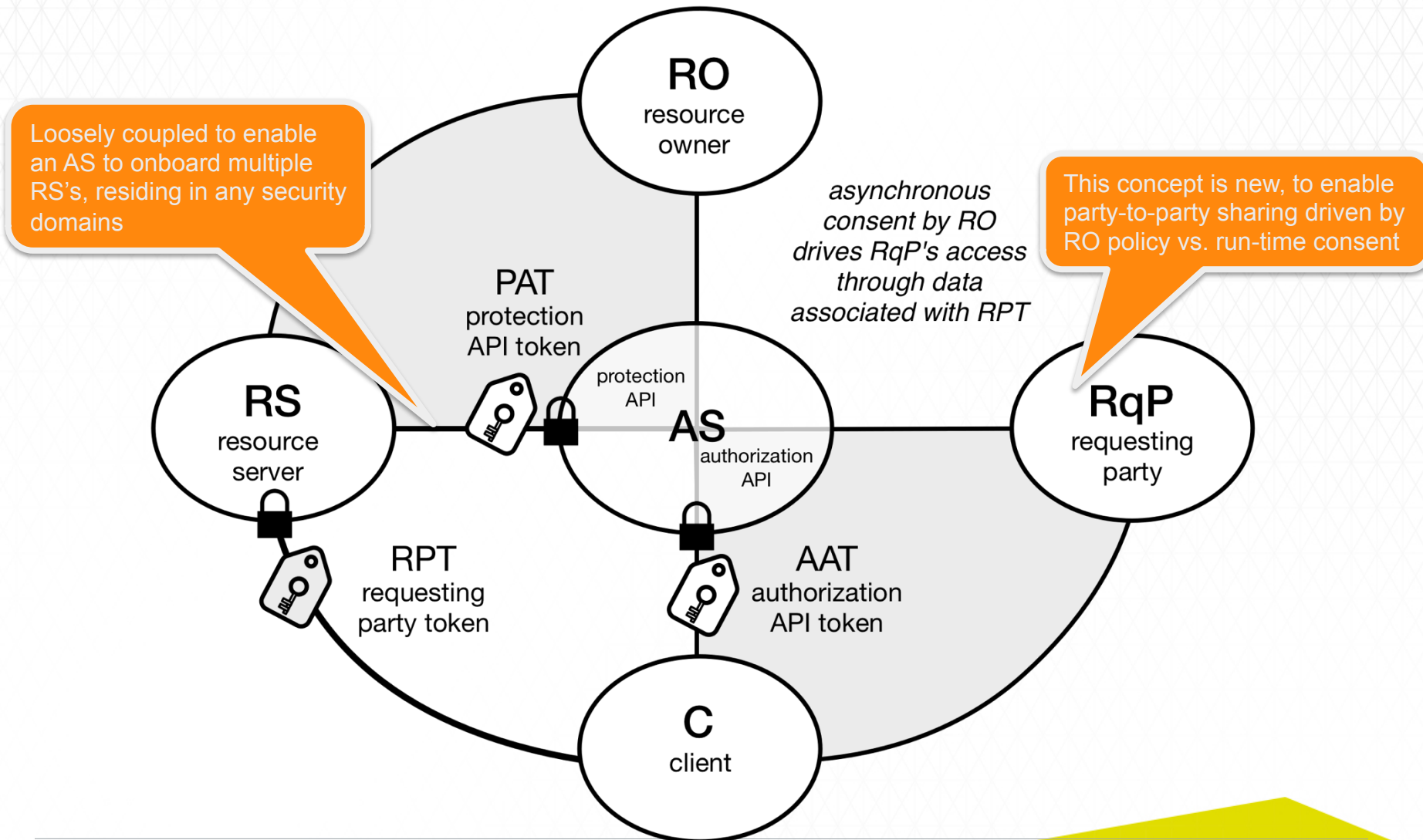
What you may want to know

Wondering how much you paid in taxes this year? This is the total tax you paid on your W-2.

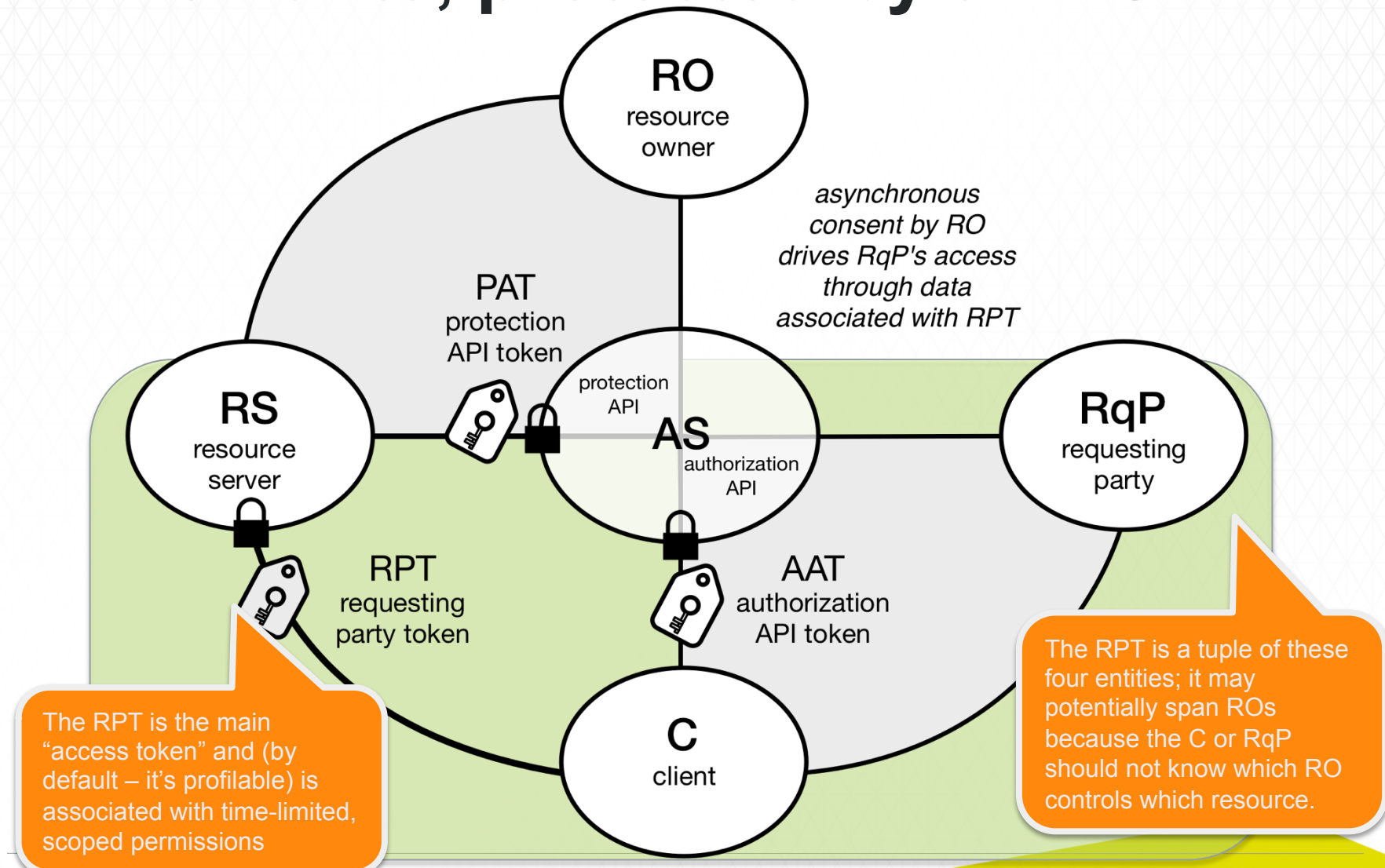
taxes from
This is the total tax
e other

deductions, like 401(k)).

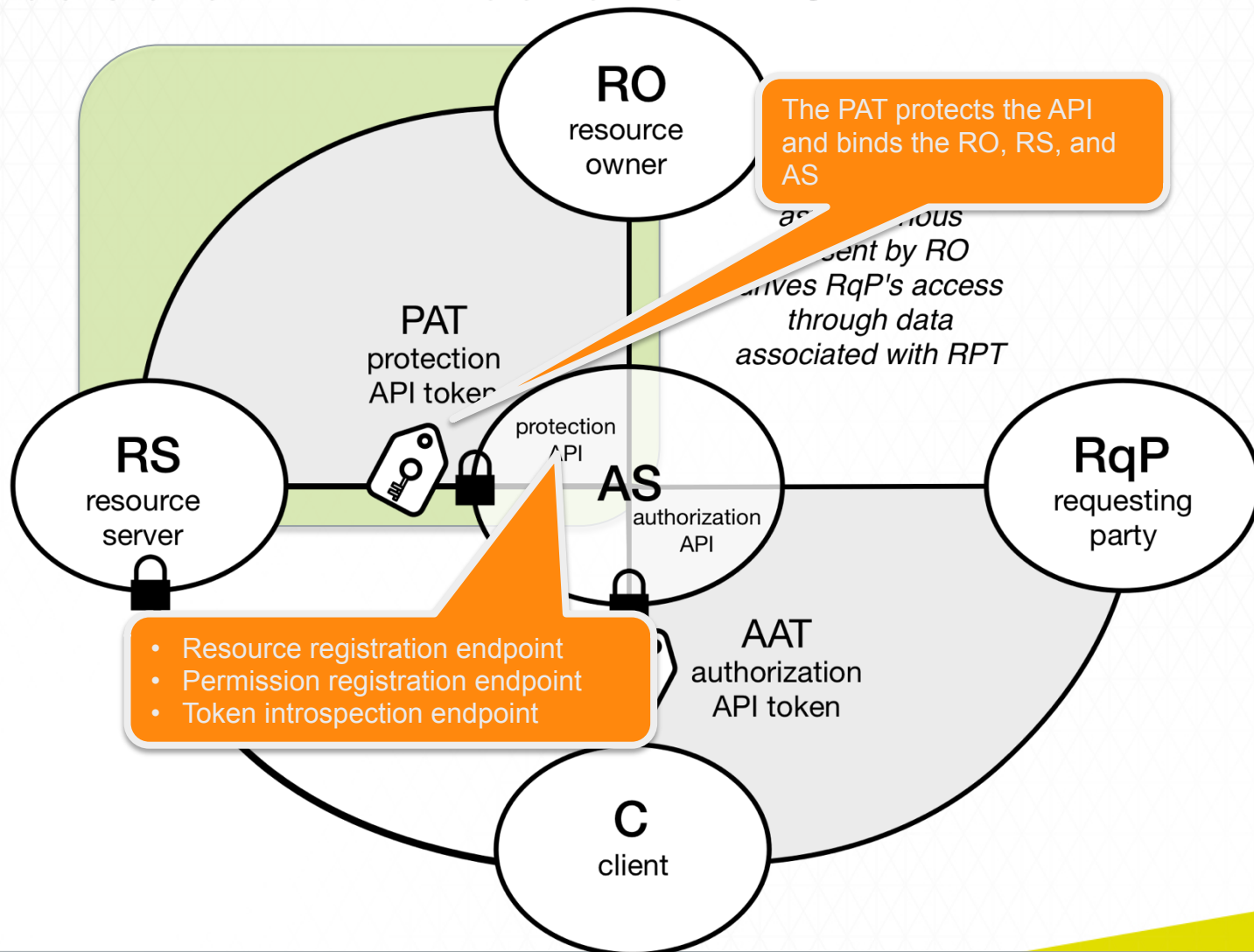
Under the hood, it's “OAuth++”



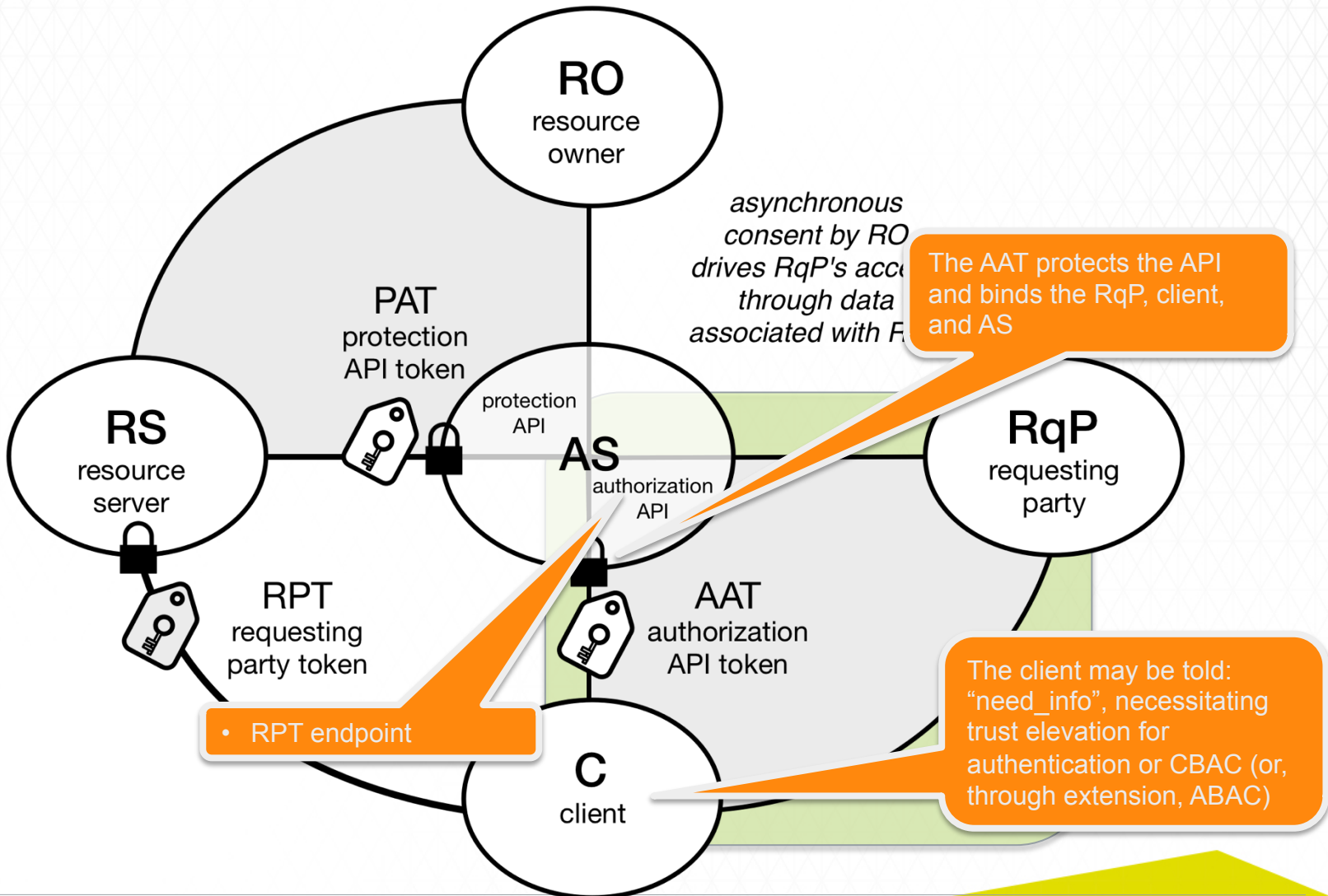
The RS exposes whatever value-add API it wants, protected by an AS



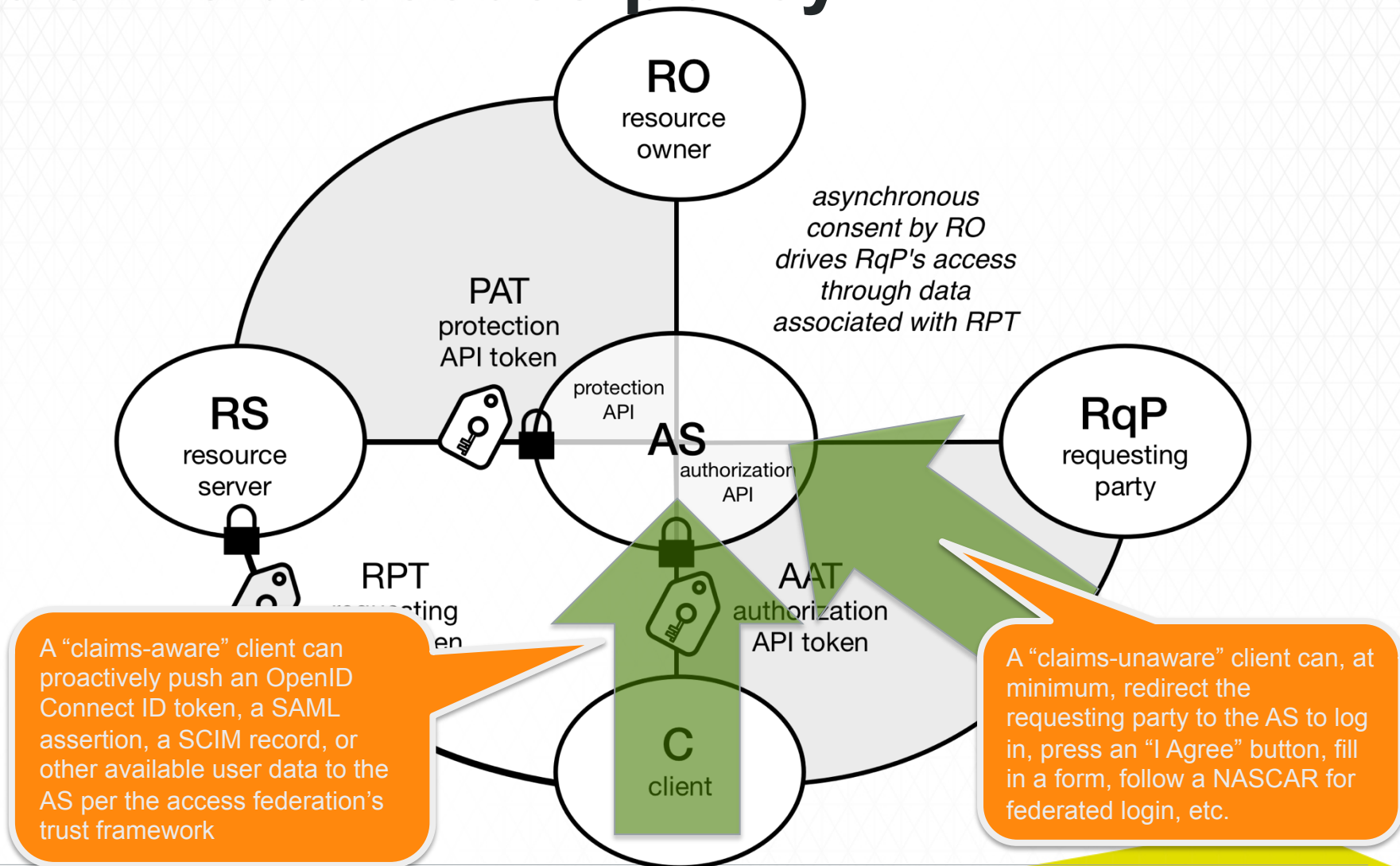
The AS exposes an UMA-standardized protection API to the RS



The AS exposes an UMA-standardized authorization API to the client

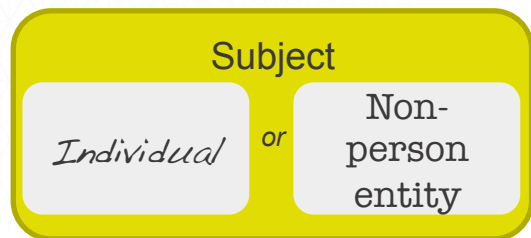


The AS can collect requesting party claims to assess policy



UMA Binding Obligations

- Distributed authorization across domains? Scary!
- This “legal” spec enables parties operating and using software entities (and devices) to distribute rights and obligations fairly in *access federation* trust frameworks



Important state changes when new pairwise obligations tend to appear:

- Token issuance
- Token status checks
- Permission registration
- Claims gathering
- Access requests
- Successful access



FORGEROCK™

Thank you!

Eve Maler

VP Innovation & Emerging Technology

eve.maler@forgerock.com

[!\[\]\(a870788d6ed9b8fd294b7654a8c8526b_img.jpg\)@xmlgrri](https://twitter.com/xmlgrri)